An Overview

Dave Mann & Matthew Wojcik

September 28, 2010

MITRE

Have you seen statements like this?

cce.mitre.org

- The required permissions for the directory %SystemRoot%\System32\Setup should be assigned
- Never add user passwords to the users.conf file through a text editor
- The "account lockout threshold" setting should be configured correctly
- Use strong passwords
- The startup type of the Remote Shell service should be set correctly

What Is CCE? – Basic Concept

- **Definition 1 – CCE assigns nominal identifiers to single configuration statements to allow for fast, accurate correlation across different tools & repositories such as:**
  - **Security guides**
  - **Benchmarks (XCCDF/OVAL)**
  - **Vendor guidance documents and documentation**
  - **Configuration Assessment tools (and manual audit reports)**
  - **Configuration Management tools**
  - **Consolidated Reporting systems**

- **EXAMPLE**
  - **CCE-2986-8**
  - **Definition: The "account lockout threshold" setting should be configured correctly**
  - **Parameters: number of attempts**

What Is CCE? – Practical Meaning

- **Definition 2 – If a configuration issue can be verified by an assessment tool or applied by configuration management system, it should be assigned a CCE id**

- **Should Get CCEs:**
  - **The required permissions for the directory %SystemRoot%\System32\Setup should be assigned**
  - **The "account lockout threshold" setting should be configured correctly**
  - **The startup type of the Remote Shell service should be set correctly**
- **Should NOT Get CCEs:**
  - **Never add user passwords to the users.conf file through a text editor**
  - **Use strong passwords**

What Is CCE? – An Example

cce.mitre.org

CCE-2116-2

Definition: The "restrict guest access to application log" policy should be set correctly.

Technical References (1 or more):

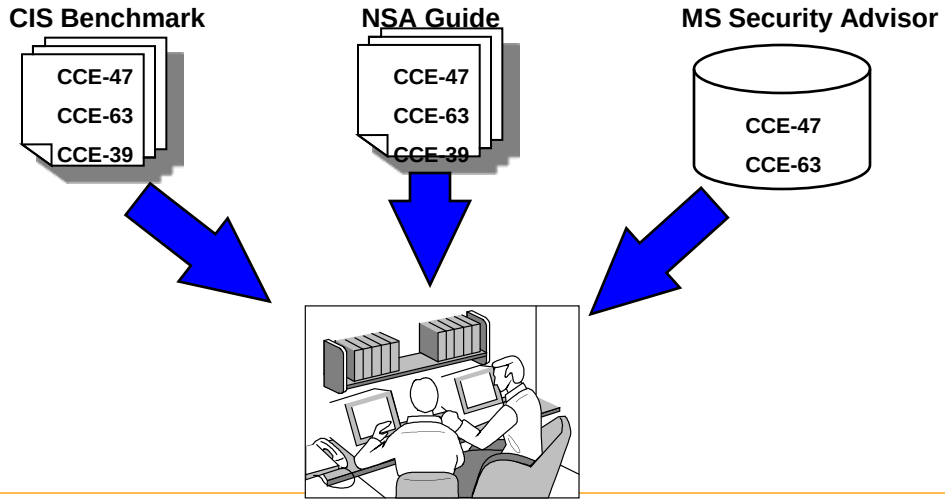
(1) HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\Application\RestrictGuestAccess
(2) defined by Group Policy

Parameters (1 or more): (1) enabled/disabled

- **Standardized Identifier - Similar to existing CVE and CME**
- **Definition - Describes the configuration control…**
  - **… but does not assert a recommendation**
- **Technical References - Describes mechanisms used to achieve the intended affect**
- **Parameter – Describes conceptual range of values**

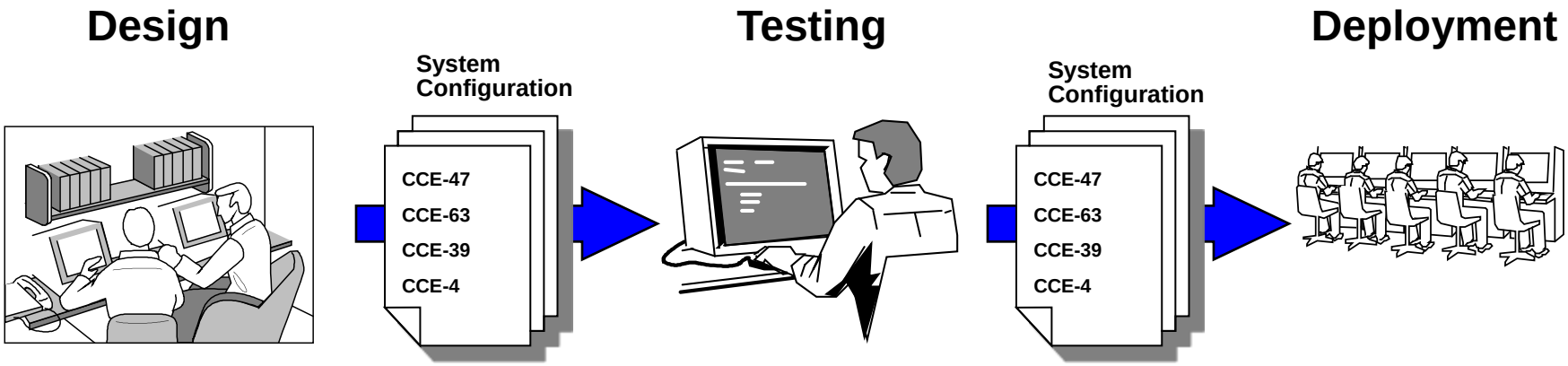
Use Case – System Design (1/5)

- **SCENARIO – System designer working to merge configuration guidance with local operational constraints. She needs to find more information about a configuration issue and its ramifications. She will look for this information in multiple sources.**
- **DISCUSSION EXAMPLES:**
  - **Use strong passwords**
  - **The "minimum password age" setting should meet minimum requirements. (CCE-2439-8)**



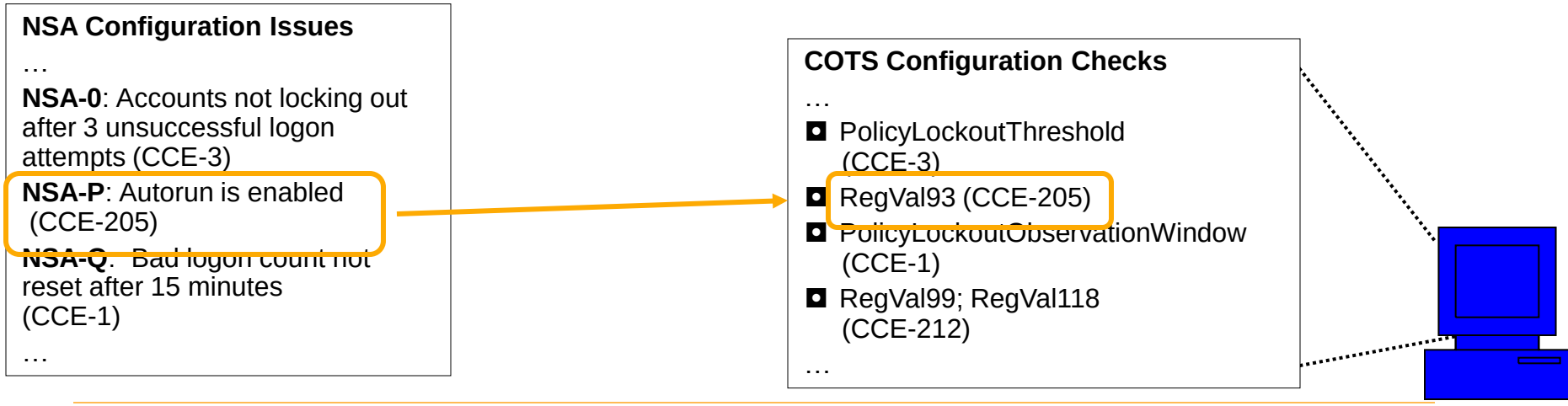
Use Case – CM Life-cycle (2/5)

- **SCENARIO – An organization has different groups responsible for system design, testing and deployment. These groups need to be able to communicate quickly and accurately about different configuration controls. Portions of these processes are becoming automated.**
- **DISCUSSION EXAMPLES:**
  - **Use strong passwords**
  - **The "minimum password age" setting should meet minimum requirements. (CCE-2439-8)**



Use Case – System Audit (3/5)

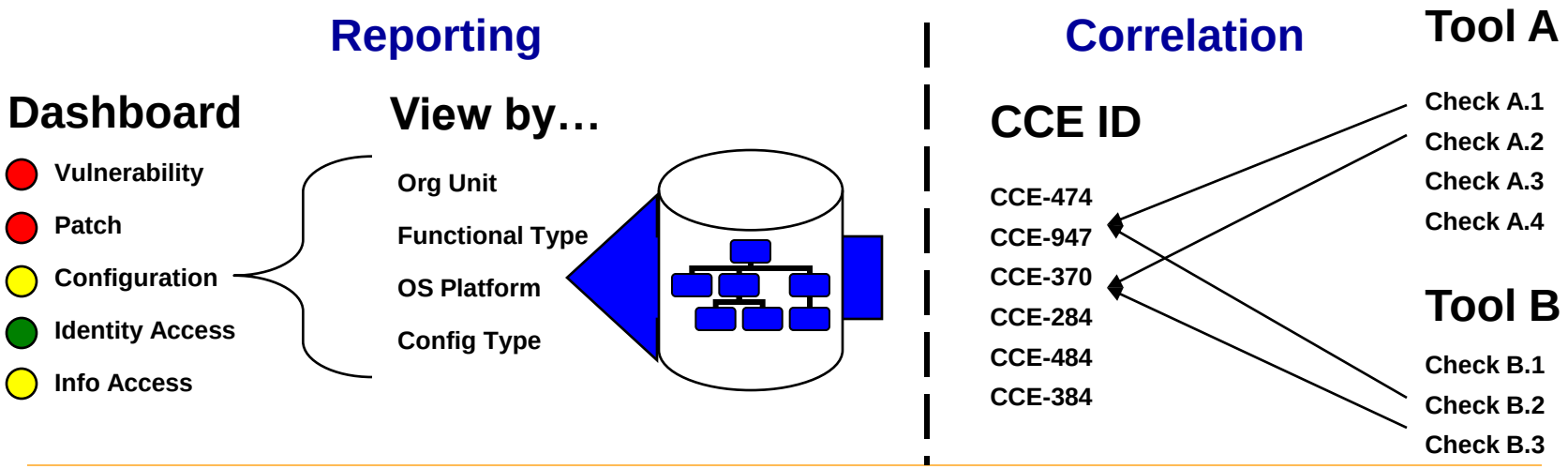
- **SCENARIO – An auditor is creating an audit plan for a system based on the security guide. He must interpret prose based statements and convert them into specific technical findings statements. When available, he must identify checks in available products that will test systems for auditable configuration settings.**
- **DISCUSSION EXAMPLE:**
  - **Windows CD Autorun**



Use Case – Data Correlation (4/5)

- **SCENARIO – A manager is responsible for consolidating system audit reports on the same platform or application based on data from multiple sources including:**
  - **Manual system audits**
  - **Commercial Assessment Products (numerous)**

  However, the configuration findings are all identified with proprietary names. Correlating the data is expensive and error prone.



Use Case – Compliance / C&A (5/5)

- **SCENARIO: A CISO or system owner must demonstrate that she has implemented appropriate configuration controls to meet regulatory or certification requirements. The relationships between requirements and controls may be many to many. Because there is no standardized way to reference controls, the auditor or certifier has difficulty understanding the system owner's control decisions and how they support the requirements.**

CCE provides common language

sp 800-53 Requirements	MAPPING	Configuration Controls
Security Requirement No. 1	1 TO 1	CCE-435
Security Requirement No. 2	1 TO MANY	CCE-246, CCE-993
Security Requirement No. 3 Security Requirement No. 4	MANY TO 1	CCE-169
Security Requirement No. 5 Security Requirement No. 6	MANY TO MANY	CCE-243, CCE-135, CCE-187

TABLE 2: SAMPLE REQUIREMENTS TRACEABILITY MATRIX

Current CCE Lists

AIX 5.3	May 6, 2009
HP-UX 11.23	May 6, 2009
Internet Explorer 7	April 28, 2010
Microsoft Office 2007	April 28, 2010
Microsoft Windows Vista	April 28, 2010
Microsoft Windows 2000	April 28, 2010
Microsoft Windows Server 2003	April 28, 2010
Microsoft Windows Server 2008	April 28, 2010
Microsoft Windows 7	April 28, 2010
Microsoft Windows XP	April 28, 2010
Red Hat Enterprise Linux 4	May 6, 2009
Red Hat Enterprise Linux 5	April 28, 2010
Sun Solaris 8	May 6, 2009
Sun Solaris 9	May 6, 2009
Sun Solaris 10	April 28, 2010

CCE In Use

- **Security Guides (documents)**
  - **Microsoft, NSA, Center for Internet Security**
- **Structured Configuration & Audit Content**
  - **NIST SCAP Content, Microsoft Security Advisor**
- **Security Configuration Tools and Capabilities**
  - **Atlantic Systems Group, BigFix (IBM), BMC Software, CA, Center for Internet Security, eEye, Fortinet, HP, LANDesk, Lumension, McAfee, Microsoft, nCircle, NetIQ, Prism, Qualys, Shavlik, SignaCert, SpaWar, Symantec, Telos, Tenable, ThreatGuard, Tripwire, Triumphant**

Calls To Action

- **Security Practitioners**
  - Utilize CCEs internally
  - Join the CCE Working Group and make requests
  - Demand CCE IDs in your Configuration tools
- **Security Guidance & Content Authors**
  - Include CCE IDs in your guidance
  - Makes your documents more usable and actionable
  - Work with the CCE team to create draft CCE entries
- **Configuration Audit and Management Tool Vendors**
  - Educate content teams on CCEs
  - Add CCE IDs to your descriptions and GUIs
  - Work with the CCE team to create draft CCE entries

Helpful Resources

- **Section 3 of the CCE white paper**
  - http://cce.mitre.org/documents/Introduction_to_CCE_White_Paper_July_2008.pdf
- **CCE List**
  - http://cce.mitre.org/lists/cce_list.html
- **CCE Working Group List**
  - cce-working-group-list@lists.mitre.org
  - Email cce@mitre.org to join list
- **CCE Team**
  - cce@mitre.org

cce.mitre.org

QUESTIONS?

cce.mitre.org

Backup Slides

MITRE

What Is CCE? – An Industry Resource

- **Definition 3 – CCE is a forum of industry experts (CCE Working Group) and lessons learned (Content Decisions) that can be leveraged by configuration management professionals to allow content to be written in manner that facilitates better technical implementation across the configuration management life-cycle**

- **Example: Use strong passwords**
  - **The "minimum password age" setting should meet minimum requirements. (CCE-2439-8)**
  - **The "minimum password length" setting should meet minimum requirements. (CCE-2981-9)**
  - **The "password must meet complexity requirements" setting should be configured correctly. (CCE-2735-9)**
  - **The "enforce password history" setting should meet minimum requirements. (CCE-2994-2)**
  - **The "store password using reversible encryption for all users in the domain" setting should be configured correctly. (CCE-2889-4)**

What Is CCE? – Parameters (5/6)

- **GOAL: Comparable configuration settings get same CCE**

- **Example: Different parameter values**
  - **Comparable statements:**
    - **DISA Gold Disk Tool for W2K:**
      Account logon lockout threshold = 3
    - **CIS Level 1 Benchmark for W2K:**
      Account logon lockout threshold = 50
  - **Unifying CCE:**
    - **CCE-3124-5 : The maximum number of failed login attempts should meet minimum requirements**
    - **Parameter: Maximum number of attempts**

What Is CCE? – Technical Mechanisms (6/6)

- **GOAL: Comparable configuration settings get same CCE**

- **Example: Different technical mechanisms**
  - **Comparable statements:**
    - **Registry Key: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\System\DisableCAD**
    - **Local Security Policy: Security Settings\Local Policies\Security Options\Interactive logon: Do not require CTRL+ALT+DEL**
    - **Group Policy Object Editor: Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options\Interactive logon: Do not require CTRL+ALT+DEL**
  - **Unifying CCE:**
    - **CCE-3886-9 : The "Disable CTRL+ALT+Delete Requirement for Logon" policy should be set correctly.**
    - **Parameter: Enabled or disabled**

Non-comparable Statements: Platform Groups

- CCE differentiates between “platform groups”
  - Typically, major releases of software
- Similar configuration statements for different platform groups are assigned different CCE ids
- Aligns with common practice in CCE communities
  - Configuration audit and management tools
  - Primary software vendors
  - Configuration guidance authors
- CCE platform groups do not align with all use cases
  - Roll-up reporting

The Guidance Life-cycle With CCE (2/2)

Guidance	Audit	Fix	Reporting
Government – Ddljkdlja – CCE-123	**Manual** – CCE-123 – Kakdwel	**Government** – Lakdkeie – CCE-123	**Tool 1** – Raleiaec – CCE-123
Vendor – Adljadoe – Dlkajde – CCE-123	**Tool 1** – Udkalkd – CCE-123 – Maakdhe	**Vendor** – Kdkdiewzl – Olkdjie – CCE-123	**Tool 2** – Dkdielse – CCE-123 – Lakejieck
3rd-Party – CCE-123 – Walakldja	**Tool 2** – Xakdkeie – CCE-123	**3rd-Party** – CCE-123 – Palalkee	
	Tool 3 – Fdkjadkie – CCE-123 – Eakldjei		

CCE Use Cases

- Guide Document Authoring and System Design
  - Relating best practice or requirements guides to deployable images
- The Configuration Management Lifecycle
  - Coordinating system design, pre-deployment testing, provisioning and deployment, configuration audit and remediation
- Configuration Tool Design and Use
  - Selecting what checks to run
- Audit Tool Result Integration
  - Correlate results from various tools from different vendors
- Regulatory Compliance
  - Establish, document, and demonstrate mappings between configurations and regulatory controls

Problem & Solution (1/2): Add Clarity to Guidance

cce.mitre.org

- **PROBLEM – Traditional configuration guidance documents lack sufficient detail to facilitate consistent technical interpretation and implementation**
- **SOLUTION – Inclusion of CCEs in guidance documents can:**
  - **Augment prose with "atomized" configuration specifics**
  - **Prompt guide authors to add configuration specifics necessary for consistent technical implementations**
  - **Provide lightweight "structure" to document configuration specifics**
- **PROSE: Use strong passwords**
- **SUPPORTING CCEs**
  - **The "minimum password age" setting should meet minimum requirements. (CCE-2439-8)**
  - **The "minimum password length" setting should meet minimum requirements. (CCE-2981-9)**
  - **The "enforce password history" policy should meet minimum requirements. (CCE-2994-2)**

Problem & Solution (2/2): Fast, Accurate Correlation

cce.mitre.org

- **PROBLEM – There is a growing need to correlate configuration data across multiple sources…**
  - **Configuration Guides (e.g. NSA, STIGs)**
  - **Vendor Documentation (e.g. MS TechNet)**
  - **System Audit Tools (e.g. DISA Gold Disk, McAfee Policy Auditor)**
  - **Configuration Management Tools (e.g. Microsoft SCCM, Tivoli)**
  - **Consolidated Reporting Tools (e.g. DISA VMS)**
- **…But it is impossible to quickly and accurately correlate configuration issues**
- **SOLUTION – Tag configuration atoms with CCE IDs**
  - **Easily added in reference fields**
  - **Common identification enables correlation**

A Brief Tour of the CCE List

Why There's Centralized Editorial Control of CCE

Examples of Flat Enumerations

- VIN – on your car
- License Plates – on your car
- SSN – on your tax forms
- Employee # - on my personnel records
- Serial Numbers - on your laptop
- Inventory Numbers – on MITRE laptops
- ISBN – on books
- Library of Congress – on books
- UPC – on books and other kinds of inventory
- CVE – for vulnerabilities
- CCE – for configuration controls
- CWE – for weaknesses? (a.k.a. vulnerabilities)
- CCI – for configuration? controls

Technical Features of Flat Enumerations

cce.mitre.org

- No item "contains" other sets of other items
  - No VIN for "FORD pick up trucks"
  - No SSN for "All people born in Vermont"
- All items are at same "level of abstraction"
- All items are instances of the same kind of category (object)
- Namespace typically has indicator of category
  - E.g. "VIN:", "SSN:", NNN-NN-NNNN, "ISBN:", (NNN) NNN-NNNN
- Identifier typically treated as nominal (non-descriptive)
  - Some identifiers may use descriptive information to generate uniqueness (often provenance information)
  - Some experts may be able to "decode" this information

Political Features of Flat Enumerations

cce.mitre.org

- Typically emerge to coordinate across strongly related but different groups with common mission goal
  - SSN: taxation and benefits
  - VIN: cars as ownable property
  - ISBN: binding revenues to publishers
  - CVE: vulnerability management life-cycle
- Typically managed by industry group or government
  - Industry group: ISBN, phone numbers, UPC
  - Government: SSN, VIN, License plates
  - Proprietary: Serial numbers, inventory tracking numbers
- Corpus typically overseen by single organization
  - List integrity
  - List publication
  - Proper use enforcement

Operational Features of Flat Enumerations

- Basic operational tasks
  - New item creation
  - Item deprecation
  - List publication
- Two common & thorny edge cases:
  - When should a "thing" be added/removed to/from the list?
  - When should two "things" be treated as seperate?
  - E.g. A totaled car, salvaged titles, new SSNs
- New item creation typically implemented federally with centralized oversight
  - E.g. ISBN, VIN, Phone Numbers
- On-going need for editorial oversight & maintenance
  - List integrity
    - E.g. fake SSNs
  - Official list publication
    - E.g. the official ISBN list

How to Contribute to CCE

CCE Submissions

- **Must be well-formatted**
  - **CCE spreadsheet, or other format by agreement**
- **May contain two types of changes:**
  - **Proposed new CCEs (Candidates)**
  - **Proposed updates to existing CCEs (Modifications)**
  - **Please differentiate!**
- **Must be organized by platform group**
  - **For new platforms, pre-coordinate with CCE team**
- **Send to cce@mitre.org, or CCE Working Group list**
  - **Email us to join Working Group**
- **Provide copy of reference document(s) to CCE team**

Candidate Submissions

- **Must describe a security configuration option which exists on the associated platform group**
- **Must be an "atomic" configuration**
  - **Unambiguous**
  - **Compound configuration options must be SPLIT**
  - **…but CCEs may have overlapping meaning**
    - **E.g. inetd enabled vs ftpd enabled**
- **Must not describe a control which already has a CCE for that platform group**
  - **Submitter must search existing CCEs: Description keywords, technical mechanisms**

Candidate Submissions continued

- If a CCE exists for another platform, reuse elements as appropriate
  - Description, parameters, technical mechanisms, etc
- Must include description, parameter, reference
  - Should include technical mechanism
  - Don't include CCE id!
- Notes to reviewers can be helpful
  - Add a column for comments, questions

Modification Submissions

- Some modifications are easy to process
  - New references, additional technical mechanisms, filling in blank parameters
  - Batch up and send to cce@mitre.org
- Some modifications require more in-depth review
  - Description changes, recasting issues (split, merge, deprecate)
  - Discuss on CCE Working Group email list
- Include CCE IDs for all modifications
- Indicate which field(s) are being changed
- If adding references, provide reference source document(s)
  - New versions of sources get new reference columns!

CCE Fields

- **Description: Clear, unambiguous explanation without asserting a recommended state**
  - **No: Set minimum password length to 12**
  - **Yes: The "minimum password length" setting should meet minimum requirements.**
  - **Should describe the effect, not the means!**
- **Parameters: Express the range of conceptual possibilities**
  - **What an organization would specify in its requirements**
  - ***Not* literal values for a particular technical mechanism**
  - **If multiple parameters seem necessary, CCE may need to be split!**
- **Technical mechanisms: Methods to effect the change**
  - **How to set or check**
  - **In spreadsheets, separate with embedded carriage returns**